

Lab 3 - Named Access List

Lab 3: Basic network security— Access-lists (named)

The physical topology is shown in Figure 17–3.

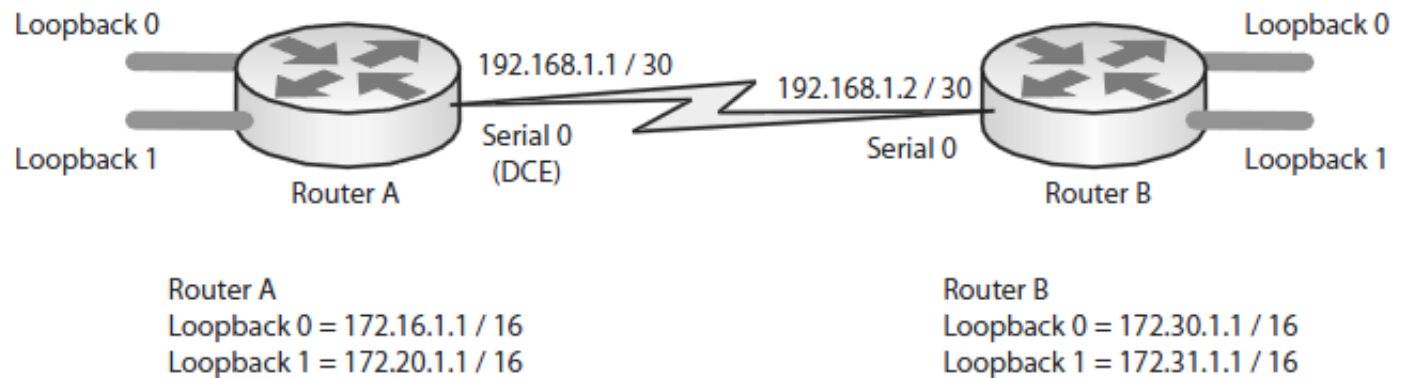


Figure 17–3: Named access-list

Lab exercise

Your task is to configure the network in Figure 17–3 to allow full connectivity using a default route. Then you will need to configure a named access-list to permit pings from loopback 0 on router B to loopback 0 on router A and telnet traffic to loopback 1 on router A only. Any other traffic will be denied (which is done by default). Please feel free to try the lab without following the lab walk-through section.

Text written in monospaced type indicates commands that can be entered on the router.

Purpose

Named access-lists are one of the foundation skills of any competent CCNA. You will be expected to be able to configure one to protect a client's network from certain types of traffic. The number one tip for access-lists is to practice over and over again and also write it out on paper in rough before you configure it (these are two tips I know).

Lab objectives

1. Use the IP addressing scheme depicted in Figure 17–3. The student who is using router A needs to configure a clock rate on interface serial 0: set this to 64000.
2. Set telnet access for the router to use the local login permissions of username "banbury" and the password "ccna".
3. Configure the "enable password" to be "cisco".
4. Configure a default route to allow full connectivity.
5. Configure an access list on Router A to permit ICMP from 172.30.1.1 to 172.16.1.1 and telnet to 172.20.1.1 only.
6. Finally, to test that the access-list is working you will need to telnet to your neighbor's

router.

Lab walk-through

1. To set the IP addresses on an interface, you will need to do the following:

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#interface serial 0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.252
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#interface loopback 0
RouterA(config-if)#ip address 172.16.1.1 255.255.0.0
RouterA(config-if)#interface loopback 1
RouterA(config-if)#ip address 172.20.1.1 255.255.0.0
RouterA(config-if)# ^ Z
RouterA#
```

Router B:

```
Router#config t
Router(config)#hostname RouterB
RouterB(config)#interface serial 0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.252
RouterB(config-if)#no shutdown
RouterB(config-if)#interface loopback 0
RouterB(config-if)#ip address 172.30.1.1 255.255.0.0
RouterB(config-if)#interface loopback 1
RouterB(config-if)#ip address 172.31.1.1 255.255.0.0
RouterB(config-if)# ^ Z
RouterB#
```

2. To set the clock rate on a serial interface (DCE connection only), you need to use the “clock rate #” command on the serial interface, where # indicates the speed:

```
RouterA(config-if)#clock rate 64000
```

Ping across the serial link now.

3. To set telnet access, you need to configure the VTY lines to allow telnet access. To do this type (from configuration mode):

RouterA(config)#line vty 0 4 « **Enters the VTY line configuration**

RouterA(config-line)#login local « **This will use local usernames and passwords for telnet access**

RouterA(config-line)#exit « **Exit the VTY config mode**

RouterA(config)#username banbury password ccna « **Creates username and password for telnet access (login local)**

Router B:

RouterB(config)#line vty 0 4

RouterB(config-line)#login local

RouterB(config-line)#exit

RouterB(config)#username banbury password ccna

4. To set the “enable password”, do the following:

RouterA(config)#enable secret cisco « **Sets the “enable password” (encrypted)**

Router B:

RouterB(config)#enable secret cisco

To configure a default route, there is one simple step (from configuration mode):

RouterA(config)#ip route 0.0.0.0 0.0.0.0 serial 0 « **For all unknown addresses**

send the packet out of serial 0

Router B:

RouterB(config)#ip route 0.0.0.0 0.0.0.0 serial 0

5. To configure an access-list there are two steps: first, specify the networks and traffic to permit or deny and second, apply the access-list to an interface:

```
RouterA#config t
```

```
RouterA(config)#ip access-list extended secure_LAN « Go into names
```

```
access-list config
```

```
RouterA(config-ext-nacl)#permit icmp host 172.30.1.1 host 172.16.1.1
```

```
RouterA(config-ext-nacl)#permit tcp any host 172.20.1.1 eq telnet
```

```
RouterA(config-ext-nacl)#exit
```

```
RouterA(config)#interface serial 0
```

```
RouterA(config-if)#ip access-group secure_LAN in « Assign the
```

access-list to the interface and the direction of traffic to be checked

Router B:

To test this access-list you will need to telnet to your neighbor's router: if the access-list is working the connection will be denied:

```
RouterB#telnet 192.168.1.1 « Telnet to the serial interface
```

```
Trying 192.168.1.1 ...
```

```
% Destination unreachable; gateway or host down
```

```
RouterB#telnet 172.20.1.1 « Telnet to loopback 1 will work
```

```
Trying 172.20.1.1 ... Open
```

User Access Verification

Password:

Now test the ICMP deny statement by pinging loopback 0 from the serial on router B.

```
RouterB#ping 172.16.1.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

```
U.U.U
```

Success rate is 0 percent (0/5)

```
RouterB# s
```

Now, ping from source interface 172.30.1.1, which should be permitted.

```
RouterB#ping
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.30.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
```

Show runs

```
RouterA#show run
```

```
Building configuration...
```

```
Current configuration : 831 bytes
```

```
!
```

```
version 12.1
```

```
no service single-slot-reload-enable
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
no service password-encryption
```

```
!
```

```
hostname RouterA
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
interface Loopback0
```

```
ip address 172.16.1.1 255.255.0.0
!
interface Loopback1
ip address 172.20.1.1 255.255.0.0
!
interface Ethernet0
no ip address
shutdown
!
interface Ethernet1
no ip address
shutdown
!
interface Serial0
ip address 192.168.1.1 255.255.255.252
clockrate 64000
ip access-group secure_LAN in
!
interface Serial1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
!
ip access-list extended secure_LAN
permit icmp host 172.30.1.1 host 172.16.1.1
permit tcp any host 172.20.1.1 eq telnet
!
line con 0
line aux 0
line vty 0 4
password cisco
```

login

!

end

RouterA#

RouterB#show run

Building configuration...

Current configuration : 574 bytes

!

version 12.2

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RouterB

!

ip subnet-zero

!

interface Loopback0

ip address 172.30.1.1 255.255.0.0

!

interface Loopback1

ip address 172.31.1.1 255.255.0.0

!

interface Serial0

ip address 192.168.1.2 255.255.255.252

!

interface Serial1

no ip address

shutdown

!

```
interface TokenRing0
  no ip address
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
!
end

RouterB#
```



© 2006-2011 HowtoNetwork.net All Rights Reserved. Reproduction without permission prohibited.